УДК 681.3.06

СОКОЛОВ А.В.

КОНСТРУКТИВНЫЙ МЕТОД СИНТЕЗА НЕЛИНЕЙНЫХ *S*-БЛОКОВ ПОДСТАНОВКИ, СООТВЕТСТВУЮЩИХ СТРОГОМУ ЛАВИННОМУ КРИТЕРИЮ

Одесский национальный политехнический университет,
Украина, Одесса, 65044, пр. Шевченко 1

Аннотация. Предложен конструктивный метод синтеза криптографических *S*-блоков подстановки, которые удовлетворяют одновременно как строгому лавинному критерию, так и критерию высокой нелинейности, причем в качестве исходного материала используются *S*-блоки подстановки меньшей длины и высоконелинейные бент-функции. Разработаны эффективные алгоритмы размножения полученных *S*-блоков подстановки

Ключевые слова: *S*-блок подстановки; строгий лавинный критерий; критерий высокой нелинейности

Основными характеристиками современных блочных шифров и хэш-функций, от которых зависит уровень их защищенности, являются нелинейность и лавинный эффект. Высокое значение нелинейности шифра и хороший лавинный эффект достигаются за счет применения нелинейных преобразований — криптографических *S*-блоков подстановки, качество которых определяет защищенность криптопреобразования в целом.

S-блок подстановки — это табличная подстановка, при которой группа входных битов x_i отображается в группу выходных битов y_i в соответствии с некоторым правилом, определяемым кодирующей Q-последовательностью.

Например, пусть задана кодирующая Q-последовательность длины $N = 8$

$$Q = \{4\,7\,2\,6\,1\,5\,0\,3\}, \qquad (1)$$

тогда структурная схема соответствующего *S*-блока подстановки имеет вид, приведенный на рис. 1.

Каждый *S*-блок подстановки может быть представлен в виде $k = \log_2 N$ таблиц истинности компонентных булевых функций. Например для *S*-блока подстановки (1) таблицы истинности компонентных булевых функций ($k = 3$) имеют вид, представленный в таблице 1.

Таблица 1

Q	4	7	2	6	1	5	0	3
F_0	0	1	0	0	1	1	0	1
F_1	0	1	1	1	0	0	0	1
F_2	1	1	0	1	0	1	0	0

В качестве меры нелинейности *S*-блоков подстановки обычно используют расстояние нелинейности N_S в смысле максимума минимального расстояния Хэмминга от каждой его компонентной булевой функции F_i до каждой из аффинных функций [1]

Электронный вариант статьи: http://radio.kpi.ua/article/view/S0021347013080049